CLAIMS

1. Access control method controlling access to a broadcast digital dataflow previously scrambled using an encryption key CW transmitted in encrypted form in an entitlement control message ECM also including at least one access control criterion CA, said numeric data possibly being recorded as such in a receiving terminal or decrypted during transfer, characterised in that the method includes the following steps:

on transmission:

- generating an entitlement control message R-ECM_c for recording the content of the flow as a function of a recording key KR_c and at least one criterion CRR defining a right to record,

- generating an entitlement control message P-ECM_c controlling access to play back the content of the recorded flow as a function of a playback key KP_c and at least one criterion CRP defining a right to play back, and

on reception:

- analysing the message R-ECM_c, and

- authorising the recording if the criterion CRR is verified, otherwise prohibit recording,

- analysing the message P-ECM_c, and

- authorising the playback if the criterion CRP is verified, otherwise prohibit the playback.

2. Method set forth in claim 1, characterised in that the keys CW, KR_c and KP_c are encrypted by a first service key K_s.

3. Method set forth in claim 1, characterised in that the keys CW, KR_c and KP_c are encrypted by three different service keys, namely K_S, K_{SR} and K_{SP} respectively

4. Method set forth in either claim 2 or 3, characterised in that the sending phase includes the following steps:

for each dataflow:

- breakdowning the scrambling period into a sequence of crypto-periods CP_i each defining a validity duration of an individual key CW_i, and at each crypto-period change,

- scrambling the content of the flow using the key CW_i, and memorise a value p(i) representative of the parity of i,ing an entitlement control message $SC\text{-}ECM_i$ as a function of the previously defined encryption keys CW_{i-1}, CW_i, CW_{i+1}, the value p(i) and the criterion CA_i, said message $SC\text{-}ECM_i$ being intended to transport access rights to a data segment S_i corresponding to at least two crypto-periods,

- encrypting the keys CW_{i-1}, CW_i, CW_{i+1} using the playback key KP_c,

- encrypting the result of the encryption in the previous step using a second service key K'_s,

- encrypting the result of the encryption in the previous step using the recording key KR_c.

5. Method set forth in either claim 2 or 3, characterised in that the sending phase includes the following steps:

for each dataflow:

- breakdowning the scrambling period into a sequence of crypto-periods CP_i each defining a validity duration of an individual key CW_i, and at each crypto-period change,

- scrambling the content of the flow using the key CW_i, and memorise a value p(i) representative of the parity of i,

- calculating an entitlement control message SC-ECM_i as a function of the previously defined encryption keys CW_{i-1}, CW_i, CW_{i+1}, the value p(i) and the criterion CA_i, said message SC-ECM_i being intended to transport access rights to a data segment S_i corresponding to at least two crypto-periods,

- encrypting the keys CW_{i-1}, CW_i, CW_{i+1} using a second service key K'_s,

- encrypting the result of the encryption in the previous step using the key KP_c,

- encrypting the result of the encryption in the previous step using the recording key KR_c.

6. Method set forth in either claim 4 or 5, characterised in that the emission phase also includes the following steps:

- calculating the entitlement control message $ECM_i = f[(ECW_i, OCW_i, CA)]$ wherein ECW_i and OCW_i represent the even and odd control words previously encrypted using a first service key K_s, respectively,

ECWi=CWi if i is even, otherwise ECWi=CWi+1;

$OCW_i=CW_i$ if i is odd, otherwise $OCW_i=CW_{i+1}$;

- broadcasting parameters in the ECM signal, identifying the ECM channels attached to the service broadcasting the content of messages ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$,

- providing the ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ messages to the receiving terminal.

7. Method set forth in claim 6, characterised in that the ECM_i, $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ messages are broadcast on ECM channels associated with the content of segment S_i.

8. Method set forth in claim 6, characterised in that the R-ECM message is output to the receiving terminal on request from an Authorisation Server at the network entry.

9. Method set forth in claim 6, characterised in that the P-ECM message is output to the receiving terminal on request from an Authorisation Server at the network entry.

10. Method set forth in claim 7, characterised in that the reception phase includes the following steps:

- recovering the ECM channel from the ECM_i message, using the signal attached to the service broadcasting the dataflow, and at each change of i,

- analysing the message ECM_i so as to recover the even control word OCW and the odd control word ECW, to

descramble the content of the broadcast flow so as to obtain direct access to this content.

11. Method set forth in claim 7, characterised in that the reception phase includes the following steps:

- recovering the ECM channel from the $P\text{-}ECM_c$, $R\text{-}ECM_c$, $SC\text{-}ECM_i$ messages, from the signal attached to the service broadcasting the content;

- analysing the $R\text{-}ECM_c$ message to verify record access criteria CRR,

- memorising the recording key KR_c;

- recovering the message $P\text{-}ECM_c$ and store it with the content; and

for each crypto-period i:

- recovering the message $SC\text{-}ECM_i$,

- decrypting the message $SC\text{-}ECM_i$ using the recording key KR_c, and

- recording the decrypted message $SC\text{-}ECM_I$ with the content.

12. Method set forth in claim 7, characterised in that playback access to the content in the recorded flow is obtained according to the following steps:

- recovering the message $P\text{-}ECM_c$ in the content and analyse it to verify read access criteria CRP,

- memorising the playback key KP_c; and

- recovering the current $SC\text{-}ECM_i$ message in the content;

- decrypting the $SC\text{-}ECM_i$ message with the playback key KP_c and verify access criteria,

- recovering the encrypted keys CW_{i-1}, CW_i, CW_{i+1} and the value p(i) indicating the parity of i, and

- decrypting said keys depending on the read direction to deduce ECW and OCW from them; then

- applying either ECW or OCW to descramble the content when playing back.

13. Method set forth in claim 7, characterised in that access to play back the content of the flow is obtained according to the following steps:

- recovering the message $P\text{-}ECM_c$ in the content,

- analysing the message $P\text{-}ECM_c$ to verify read access criteria CRP,

- memorising KP_c, and

- recovering the current $SC\text{-}ECM_i$ message in the content,

- decrypting the $SC\text{-}ECM_i$ message with the second service key K'_s and verify access criteria,

- recovering the encrypted keys CW_{i-1}, CW_i, CW_{i+1} and the value p(i) indicating the parity of i, and

- decrypting said keys depending on the direction of reading to deduce ECW and OCW; then

- applying either ECW or OCW to descramble the content.

14. Method set forth in either claim 11 or 12, characterised in that the reception phase also includes the following steps:

- generating a local key K_I from attributes contained in the message R-ECM and at least one

parameter related to the identity of the receiving terminal,

- locally over-encrypting the content to be recorded with this key K_I.

- when playing back, regenerating the key K_I using attributes contained in the message P-ECM and at least one parameter related to the identity of the receiving terminal,

- decrypting the recorded content using the regenerated key K_I.

15. Method set forth in one of claims 1 to 14, characterised in that the broadcast digital data represent audiovisual programs.

16. Access control system controlling access to a digital dataflow including a scrambling platform (2) including at least one generator of entitlement control messages ECM and at least one descrambling receiver (4) provided with a security processor (14), characterised in that the scrambling platform (2) also includes:

- a generator of entitlement control messages R-ECM_c when recording the content of the received flow and a generator of entitlement control messages P-ECM_c when playing back the content of a recorded flow, and in that the descrambling receiver (4), includes:

- means of recovering the ECM channel from P-ECM_c, R-ECM_c messages,

- means of decrypting the content of a received flow to record it, and

- means of decrypting the content of a recorded flow to play it back.

17. System set forth in claim 16, characterised in that the descrambling receiver (4) also includes means of generating a local key K_I from attributes contained in the R-ECM_c message and the identity of the receiving terminal to locally encrypt/decrypt the content of the received flow.

18. Scrambling platform (2) including at least one generator of entitlement control messages ECM controlling access to a dataflow broadcast in scrambled form, characterised in that it also includes a generator of entitlement control messages R-ECM_c to control recording the content of a received flow and a generator of entitlement control messages P-ECM_c to control play back the content of a recorded flow.

19. Scrambling platform set forth in claim 18, characterised in that it includes:

- means of breaking down the scrambling period into a sequence of crypto-periods CP_i each defining a validity duration of an individual key CW_i,
- means of encrypting the content of the flow at each change of the crypto-period i using the key CW_i,
- means of calculating an entitlement control message SC-ECM_i as a function of the keys CW_{i-1}, CW_i, CW_{i+1} corresponding to crypto-periods CP_i, CP_{i-1} and CP_{i+1} respectively, a parity parameter p(i) and the access control criterion CA_i, said message SC-ECM_i being

intended to carry access rights to a data segment S_i corresponding to at least two crypto-periods,

- means of encrypting the keys CW_{i-1}, CW_i, CW_{i+1} using a playback key KP_c,

- means of encrypting the encryption result in the previous step using a second service key K'_s,

- means of encrypting the result of the encryption in the previous step using a record key KR_c.

20. Platform set forth in claim 18, characterised in that it also includes:

- means of breaking down the scrambling period into a sequence of crypto-periods CP_i each defining a validity duration of an individual key CW_i,

- means of encrypting the content of the flow at each change of the crypto-period i using the key CW_i,

- means of calculating an entitlement control message $SC\text{-}ECM_i$ as a function of the keys CW_{i-1}, CW_i, CW_{i+1} corresponding to crypto-periods CP_i, CP_{i-1} and CP_{i+1} respectively, a parity parameter p(i) and the access control criterion CA_i, said message $SC\text{-}ECM_i$ being intended to carry access rights to a data segment S_i corresponding to at least two crypto-periods,

- means of encrypting the encryption result in the previous step using a second service key K'_s,

- means of encrypting the control words CW_{i-1}, CW_i, CW_{i+1} using a playback key KP_c,

- means of encrypting the encryption result in the previous step using a record key KR_c.

21. Descrambling receiver (4) of a dataflow broadcast in scrambled form using a scrambling key CW_i including a security processor including at least one key KR_c intended to descramble record entitlement control messages $R\text{-}ECM_c$ and at least one key KP_c intended to descramble the play back entitlement control messages $P\text{-}ECM_c$, receiver characterised in that it includes:

- means of recovering the ECM channel from $P\text{-}ECM_c$ messages, and $R\text{-}ECM_c$ messages from the signal attached to the service broadcasting the content;
- means of decrypting messages $R\text{-}ECM_c$ using the record key KR_c to verify the right to record the content of a received flow,
- means of decrypting messages $P\text{-}ECM_c$ using the key KP_c to verify the right to play back the content of a recorded flow.

22. Receiver set forth in claim 21, characterised in that it also includes means of generating a local key K_I from attributes contained in the receiver identity message R-ECM and locally decrypt the content of the received flow.

23. Receiver set forth in claim 21, characterised in that the security processor is a smart card.